REMARKS

Applicant has carefully studied the outstanding Official Action. The present amendment is intended to be fully responsive to all points of rejection and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the present application are hereby respectfully requested.

Prior to the present amendment the application comprised outstanding claims 84 - 122, 124 - 140, and 153 - 186.

The Examiner requested that Figs. 1 and 2 should be designated by a legend such as "Prior Art", in accordance with MPEP 608.02. As such, Applicant hereby respectfully submits the enclosed replacement drawings with the present response.

Claim 165 stands objected to as claim 165 recites the variable r, without providing any explanation as to the definition of r. Claim 165 has been cancelled, as discussed below.

Claims 171 and 172 stand objected to as they recite the limitation "the second end user device", which lacks antecedent basis. Claims 171 and 172 have, accordingly, been amended to recite "the end user device".

Claims 105 - 110 and 171 - 175 stand rejected under 35 USC 102(e) as being anticipated by Maillard, US 6,393,562.

Maillard describes a receiver/decoder programmed only to accept a current entitlement control message (EMM) if it has received at least a previous EMM of a previous calendar period. When the EMM is received, it is used to check present rights in the receiver/decoder.

The Examiner's rejection of claim 105 includes the following portion: "transmitting a PECM (**EMM** [sic]) to the end user by said control center, said PECM being specific to the end user device - [Maillard] Col. 3, lines 46 - 55". The lines of Maillard cited state: "According to another aspect of the invention, there is provided a transmitter for use in a method of preventing fraudulent access in a conditional access system which is linked to the subscriber's receiver/decoder

for receiving an entitlement management message (EMM) for a group of subscribers to enable said system to provide access for a respective subscriber, the receiver/decoder being programmed only to accept a current EMM of a calendar period if it has received at least a previous EMM of a previous calendar period."

Applicant respectfully points out that the Examiner seems to be confusing PECMs and EMMs. PECMs are a type of ECM, and are similar to the TECMs described in Published European Patent Application EP 0858184 (incorporated in the present application by reference at page 5, lines 5 - 7), which corresponds to US Patent 6,178,242. The following is a quote from EP 0858184 (column 9, line 43 - column 10, line 36):

> The IRD 110 of FIG. 1, in cooperation with the smart card 120, is preferably operative to process the broadcast SDDS 140, in order to produce a recording SDDS 165, as follows. Each ECM, such as the nth ECM 145, is processed as described above, typically using an ECM key, which may comprise a one-way function as described above, the ECM key being known to the smart card 120, in order to obtain the associated CW such as an nth CW 170. The nth CW 170 is then processed using another key, referred to throughout the present specification and claims as a TECM key, in order to produce an nth TECM 175 which may later be used, with the TECM key, to generate the nth CW 170.
>
> Preferably each TECM, such as, for example, the nth TECM 175, is also signed with an appropriate digital signature, as is well known in the art. Preferably, each TECM key is associated with a unique digital signature. Preferably, upon subsequent playback and descrambling of the recording SDDS 165 the digital signature is checked, and only a valid digital signature indicating that the recording SDDS 165 was produced with the apparatus of FIG. 1, typically particularly with the smart card 120 of FIG. 1, will be descrambled by the apparatus of FIG. 1. The use of such a digital signature is considered preferable in order to discourage

unauthorized duplication and subsequent playback of the recording SDDS 165 using apparatus other than the apparatus of FIG. 1, particularly using a different smart card at some other location in place of the smart card 120.

The TECM key may be of similar type to the ECM key such as, for example, a one-way function. The TECM key, however, is preferably permanently associated with the system of FIG. 1; particularly, the TECM key does not change even when the smart card 120 is replaced by the system operator, as described above. Thus, it will be appreciated that any SDDS associated with the TECM key may still be descrambled using the apparatus of FIG. 1 even after such a replacement of the smart card 120. It is appreciated that the TECM key may be produced in a wide variety of ways, such as, for example, the TECM key may be associated with and, typically, stored in the IRD 110; the smart card 120; a combination of the IRD 110 and the smart card 120, such as partly in the IRD 110 and partly in the smart card 120; or another portion of the system of FIG. 1 (not shown). It is also appreciated that the TECM key may be personal to a particular user of the apparatus of FIG. 1, with more than one TECM key being associated with the apparatus of FIG. 1 and the appropriate TECM key being produced upon identification of a user of the apparatus of FIG. 1 by any method well known in the art, such as by provision of a personal identification number (PIN).

Applicant respectfully points out that while it is true that the TECM of EP 0858184 (corresponding to the PECM of the present application) contains information used to generate a control word, the PECM / TECM is a type of ECM, and is not an EMM.

Applicant further respectfully calls the Examiner's attention to:

EP 0858184 Col. 2 line 57 - Col. 3 line 20, particularly, Col. 3, line 12 - 14, which states: "replacing each of the plurality of ECMs with a corresponding **transformed ECM** (TECM)" (emphasis added);

Page 5 of the present application, lines 16 - 23, particularly lines 21 - 22, which state: "(c) transmitting a PECM (**personal ECM**) to the end user device" (emphasis added); and

Page 9 of the present application, lines 28 - 32, particularly lines 30 - 31, which state: "Most preferably, this capability is distributed through a PECM (**personal ECM**)" (emphasis added).

Applicant respectfully points out that in all of the above cited locations, it is clear that the object of the discussion is a type of ECM and not an EMM.

The EMM of Maillard comprises a key used to decrypt all ECMs received in a month. The PECM recited in claim 105 is used to produce a control word to descramble video. At most, it would seem that the EMM of Maillard corresponds to the TECM key of EP 0858184, and not to the TECM of EP 0858184, nor to the PECM of the present invention.

In order to make the distinction between the present invention, as claimed in claim 105, and Maillard particularly clear, claim 105 has been amended to recite: "<u>said PECM including control word generating information and being associated with a PECM key for producing a control word from said PECM</u>".

The amendment is supported, inter-alia, by pages 9 - 10 of the application.

Claim 105 is therefore deemed allowable.

Claims 106 - 110 are all also rejected under 35 USC 102(e) in light of Maillard.

All of claims 106 - 110 depend, either directly, or indirectly on claim 105, and recite additional patentable material.

Thus, claims 106 - 110 are deemed allowable, with reference to the above discussion of the allowability of claim 105.

Furthermore, regarding claim 110, the Examiner rejected claim 110 citing Maillard col. 2, lines 40 - 57:

> An Entitlement Management Message or EMM is a message designated to one subscriber or to a group of subscribers. It is usually generated by a subscription authorisation system and is multiplexed with an MPEG-2 stream. It is usually encrypted with a so-called "management" key for example for group use. Hence it may be encrypted by a key common to all subscribers in a group of subscribers.

Again, Applicant respectfully points out that the Examiner is introducing confusion between a PECM and an EMM. In the first place, Maillard itself discloses changing EMMs from one month to the next (see Maillard Figs. 4 - 6 and 8, as well as the description therein of those figures). In the second place, nowhere does the section cited above recite "**permanently** associating said PECM" (or EMM, as per the Examiner, after Maillard) "with said scrambled digital content to permit unscrambling of said scrambled digital content by the end user device."

Claim 110 is therefore deemed additionally allowable in light of the above discussion, as well.

Claims 171 - 175 are all also rejected under 35 USC 102(e) in light of Maillard.

The Examiner rejected claim 171 on the basis of Maillard, Background of the Invention, Paragraph 1. Maillard, Background of the Invention, Paragraph 1, in fact states:

> In existing broadcasting systems using MPEG, in order to reduce bandwidth required to send the monthly subscriber authorisation (EMM) messages, it is customary to use a group renewal EMM, encrypted by a group management key Kg common to all subscribers in the group. As shown in FIG. 4, the EMM proper includes a subscriber bitmap 3100, typically of 256 bits. Each bit of the bitmap corresponds to a subscriber. In the example given, bit #3 corresponds to subscriber #3. The EMM proper

also includes a rights section 3102 detailing the subscription rights of all the subscribers in the group for that month and including the ECM key for that month and typically the following month. Assuming the subscriber has correctly paid his subscription for January, the presence of a positive bit 1 at this position will indicate to the subscriber's decoder (after he has decrypted the message with key Kg) that the subscriber is indeed entitled to receive programmes in this group as defined by the subscription rights section. Individual programmes are descrambled using effectively an ECM decrypted using the ECM key.

Nowhere in the cited paragraph does Maillard indicate that there is **embedding** of the ECM (or PECM) in content. Neither does Maillard indicate that there is a second device, which receives said content.

Claim 171, by contrast, recites:

"The method according to claim 105 and wherein the ECM remains **embedded** in the digital content after the receipt of the PECM at the **second end user device**." (emphasis added)

Furthermore, claim 171 depends from claim 105 and recites additional patentable subject matter.

Claim 171 is therefore deemed allowable both in light of the above discussion as well as in light of the discussion of the allowability of claim 105.

Claims 172 - 175 depend, either directly or indirectly on claim 105, and recite additional patentable matter.

Claims 172 - 175 are therefore deemed allowable with light to the above discussion of the allowability of claim 105.

Claims 113 - 122 and claims 155 - 165 stand rejected under 35 USC 102(e) in light of US 6,069,952, to Saito et al.

Saito describes a data copyright management system comprising a database for storing original data, a key control center for managing crypt keys, copyright management center for managing data copyrights, and a communication network for connecting these sections.

Applicant does not necessarily agree with the basis of the Examiner's rejection of Claims 113 - 122 and 155 - 165. However, in order to facilitate allowance of the present application, claims 113 - 122 and 155 - 165 have been cancelled without prejudice. Applicants reserve the right to pursue claims 113 - 122 and 155 - 165 in the context of a continuing application.

Claims 84 - 90, 92 - 104, 111 - 112, 124 - 140, 166 - 170, 176 - 186 stand rejected under 35 USC 103(a) over Maillard and further in view of Saito et al.

The Examiner asserts that Maillard discloses "wherein the transmitted scrambled digital content comprises at least an embedded original entitlement control message (ECM) and playable content, the embedded original ECM controlling, at least in part, access to the scrambled digital content by the first end user" (the Examiner refers to the Background of the Invention in Maillard, as support for this assertion).

Applicant respectfully disagrees, and points out that a careful reading of the Background of the Invention in Maillard shows that Maillard does not disclose an embedded ECM, and in fact, is quite silent on the delivery mechanism of the ECM. Maillard there recites: "The EMM proper also includes a rights section detailing the subscription rights of all the subscribers in the group for that month and including the ECM key for that month and typically the following month" (Col. 6. lines 5 - 8). And also recites: "Individual programmes are descrambled using effectively an ECM decrypted using the ECM key".

Examiner cites Saito as disclosing "in a content distribution system, an authorized user can send encrypted content to an unauthorized user, at which point the unauthorized user can contact a control center to receive authorization and a decryption key for the content (Saito Col. 5 Line 20 - Col. 6 Line 63)".

A careful reading of Saito shows that, in fact, Saito is quite different from the present invention.

Saito discloses (Col. 6, line 11 - 17): "When the data M is copied to external recording medium 11 or transmitted via communication network 8, the first secret-key Ks1 and the second secret-key Ks2 in primary user terminal 4 are

disused by the copyright control program P. Therefore, in order to reuse the data M, the primary user needs to request for utilization of the data M to key control center 9 to reobtain the second secret-key Ks2".

Saito further states (Col. 6, lines 39 - 48): "A secondary user who desires secondary utilization of the encrypted data Cmks2 copied or transmitted from a primary user must present original data name or data number to copyright management center 10 via communication network 8 by secondary user terminal 5 and also present the secondary user information Iu2 to request secondary utilization of the data Cmks2 to the center 10. In this case, the secondary user further presents the uncrypted primary user information Iu1 added to the encrypted data Cmks2 in order to clarify the relationship with the primary user."

Additionally, Saito states (Col. 6, lines 56 - 63): "In secondary user terminal 5 receiving the second secret-key Ks2 and the third secret-key Ks3, the encrypted data Cmks2 is decrypted using the second secret-key Ks2 by the copyright control program P

M=D(Ks2, Cmks2)

and is secondarily utilized for display or edit operations."

Applicant respectfully points out that Saito is describing a system wherein **both** the primary and the secondary user are required to contact a control program in order to obtain a non-embedded ECM.

In fact, Saito, by teaching that the second user needs to contact the control center is teaching away from Maillard, which teaches that the second user is added to the group of subscribers receiving the EMM (Maillard Col. 6, lines 26 - 34). Thus, the combination of Saito with Maillard does not seem to be justified.

Claim 84 is therefore deemed allowable.

Claims 85 - 90, 92 - 104, and 166- 170 all depend, either directly or indirectly, from claim 84, and recite additional patentable material.

Claims 85 - 90, 92 - 104, and 166- 170 are therefore deemed allowable, with reference to the above discussion of the allowabilty of claim 84.

Claims 111 and 112 both depend, either directly or indirectly, from claim 105, and recite additional patentable material.

Claims 111 and 112 are therefore deemed allowable, with reference to the above discussion of the allowabilty of claim 105, and additionally with reference to the discussion concerning the allowability of 84.

Regarding claim 124, the Examiner, in combining Maillard and Saito, states: "It would have been obvious to the ordinary person skilled in the art at the time of the invention to employ the teaches of Saito in the content distribution system of Maillard by transferring said scrambled digital content *and the ECM directly from said first end user device to a second end user device*; etc."

Applicant respectfully points out that neither Maillard nor Saito disclose an embedded ECM, hence the limitation of transferring said scrambled digital content *and the ECM directly from said first end user device to a second end user device* is not found in the references. Neither is sending the ECM as an embedded ECM is not suggested by either of the references.

Applicant respectfully calls the Examiner's attention to MPEP, Section 2143.03, which explicitly states: "To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art."

Claim 124 is therefore deemed allowable.

Claims 125 - 140 and 176 - 180 all depend, either directly or indirectly, from claim 124, and recite additionally patentable material.

Claims 125 - 140 and 176 - 180 are all deemed allowable with reference to the above discussion of the allowability of claim 124.

Claims 181 - 186 are hereby cancelled without prejudice.

In view of the foregoing remarks, it is respectfully submitted that the present application is now in condition for allowance. Favorable reconsideration and allowance of the present application are respectfully requested.

Respectfully submitted,

CLIFFORD J. MASS
c/o Ladas & Parry LLP
26 West 61st Street
New York, New York 10023
Reg. No. 30,086
Tel. No. (212) 708-1890

IN THE DRAWINGS:

Please replace the drawing sheets of Figs. 1 and 2 on file with the enclosed replacement drawing sheets.